Serial No. 09/884,672
Art Unit No. 2134

REMARKS

Claims 1-4, 6-16, 18-28, 30-35, and 37-41 are currently pending in the patent application. The Examiner has stated that Claims 4, 6-7, 16, 18-19 and 28 are rejected under 35 USC 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which application regards as the invention. Specifically, the Examiner has concluded that the phrase "defining a numeric on which an operator operates as an input to the operator" is indefinite and the phrase "defining an operation results of the operator as an output of the operator" are unclear. Applicants have reviewed the claim language and believe that the objectionable language can be deleted from the claims without affecting the meaning or scope of the claims. While Applicants had included the language to provide antecedent basis for the input and output of each of the serial sequence of operators, the subsequent claim language recites "an input" and "an output" which would not therefore require the antecedent basis. Therefore, by this amendment, Applicants are deleting the language which the Examiner has identified as unclear from each of Claims 4, 6, 7, 16, 18, 19 and 28. Applicants request confirmation that the amendments address the Examiner's concerns.

The Examiner has rejected Claims 1, 13, 25, 30-31, and 37 as anticipated under 35 USC 102 by Vainio; has rejected Claims 2-3, 14-15 and 26-27 under 35 USC 103(a) as being unpatentable over Vainio in view of Official Notice; has rejected Claims 8 and 20 under 35 USC 103(a) as being unpatentable over Vainio in view of Schneier; has rejected Claims 4, 6-7, 16, 18-19, 28, and 32 under 35 USC 103(a) as being unpatentable over Vainio in view of Flanagan and further in view of Schneier; and, has rejected Claims 9-12, 21-24, 33-35, and 38-41 under 35 USC 103(a) as being unpatentable over Vainio in view of Schneier and further in view of David, Narayanaswami and Lin.

The Vainio reference teaches security measures for Bluetooth communications. Under the Vainio method, a "verifier" device sends a random number to a claimant device, whereupon the claimant device applies a function to the random number to generate a "SRES" response which is sent to the verifier. At the verifier device, the received SRES is compared to a locally-calculated SRES'. Applicants respectfully assert that the Vainio reference does not anticipate or obviate the invention as now claimed, alone or in combination with any of the additionally-cited art. First, the Vainio reference does not teach that two send/receive devices generate verification data and send that data to their respective output devices, after which the data are compared. Rather, Vainio requires that one device act as the verifier, to send the random number, receive the SRES, and perform the verification. Further, Vainio does not teach or suggest that a plurality of verification data values be generated and compared for mutual matches, as is claimed. While the Examiner seeks to analogize successive iterations of Vainio interactions to the claimed invention, Applicants respectfully assert that the generation of a plurality of verification data, for example for data having a plurality of divisions (see: page 23, et seq), is neither taught nor suggested (independent Claims 1, 13, 25, and 30-41, as well as the claims which depend respectively therefrom). Applicants further assert that there is nothing in Vainio which teaches or suggests the means or steps for establishing a serial sequence of operators, and letting an input to the serial sequence of operators be the data for verification (claims 4, 6, 16, 18, and 28). Applicants further assert that Vainio does not teach or suggest the means for applying and the steps for applying second generation algorithms, in addition to the first generation algorithms, to accomplish the claimed verification (Claims 9-12, 21-24, 33, and 38-41).

The Examiner has concluded that it is inherent in Vainio that the SRES values be placed in verification data output sections. Applicants respectfully assert that Vainio makes no mention of any output sections. Absent some teaching, it cannot be concluded that Vainio teaches or inherently includes such a feature. Applicants suggest, for example, that the verifier of Vainio could calculate the SRES' and compare it to SRES without ever "outputting" the SRES' value. Accordingly, inherency cannot be relied upon for the rejection.

It is well established under U. S. Patent Law that, for a reference to anticipate claim language under 35 USC 102, that reference must teach each and every claim feature. Since the Vainio reference does not teach steps or means as claimed, it cannot be maintained that Vainio anticipates the invention as set forth in the independent claims, Claims 1, 11-13, 25, and 30-41, or the claims which depend therefrom and add further limitations thereto.

The Examiner has again taken "official notice" of recited claim features. Applicants dispute the Examiner's conclusions that Vainio in view of "official notice" obviates the invention as claimed. While audio and visual prompts ("enter password now") and messages ("password not valid") may be known, Applicants contend that such prompts are not the same as nor suggestive of audible or visual verification data per se. Display of verification data is not known. What the Examiner parenthetically notes is a Windows message generated in response to entry of an invalid password; however, Windows does not display verification data (see: e.g., Fig. 5 of the present specification). Clearly, therefore, the obviousness rejections cannot be maintained.

The Examiner has rejected Claims 8 and 20 as unpatentable over Vainio in view of Schneier, acknowledging that "Vainio does not teach that the data for verification data generation is a public key of either data send/receive device." As argued above, Applicants believe that the Vainio patent does not teach or suggest the features of the claims from which Claims 8 and 20 respectively rely. While Schneier may disclose that a public key may require verification, Schneier does not provide teachings which are missing from Vainio. Schneier does not teach or suggest means or steps for generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to its own verification data output section, means or steps for generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to its own verification data output section, or means or steps for determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually, wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually. Accordingly, the combination of Vainio and Schneier does not obviate the invention as claimed.

The Examiner has rejected Claims 4, 6-7, 16, 18-19, 28 and 32 as unpatentable over Vainio in view of Flanagan and Schneier. Flanagan is cited as defining an operation result and a numeric. Since that language has been deleted from the claims by amendment, Applicants respectfully assert that the rejections based on the teachings of Flanagan are moot.

With regard to the teachings of Schneier, the Examiner has acknowledged that Vainio does not teach that the algorithm E1 is a one-way function and cited Schneier as teaching one-way functions. While Schneier presents one-way functions in the publication, Schneier does not teach, on page 29 or pages 351-353, that the one-way hash functions be used in establishing a serial sequence of operators for verification data generation, as is claimed. Applicants disagree with the Examiner's interpretation of the teachings of Schneier found on page 352 and respectfully request reconsideration of the rejections. Applicants reiterate that the combination of Vainio and Schneier does not teach or suggest means or steps for generating verification data from the sent data for verification data generation produced using a first generation algorithm and outputting the generated verification data to its own verification data output section, means or steps for generating verification data from the received data for verification data generation produced using the first generation algorithm and outputting the generated verification data to its own verification data output section, or means or steps for determining whether the verification data at the verification data output sections of both the data send/receive devices matches mutually, wherein the first generation algorithm generates a plurality of verification data, wherein for each verification data, it is determined whether the verification data at the verification data output sections of both the data send/receive devices match mutually, and further does not obviate those claim features further comprising the means and steps for providing the serial sequence of one-way functions.

With regard to the rejections of Claims 9-12, 21-24, 33-35 and 38-41 as unpatentable over Vainio in view of Schneier and further in view of Davis, Narayanaswami and Lin, Applicants again rely on the interpretation set forth above with regard to the teachings of the Vainio and Schneier references. Applicants respectfully assert that, even if one were to modify Vainio with teachings from the additionally cited references, one would not arrive at the invention as claimed. Since none of the cited references teaches or suggests means and steps for generating a plurality of verification data with first generation algorithms, for comparing the plurality of verification data, for defining functions and sequencing operators, for applying second generation algorithms, it cannot be maintained that the combination of references obviates the invention as claimed. Adding a terminal connected to a PC by a secure path from Narayanaswami or a secure path from Davis to the combined teachings of Vainio and Schneier would not yield the invention as claimed. Similarly, simply adding the Lin teachings that "computing power, memory capacity and supply power of the portable device may not be sufficient for key generation" (page 12 of Office Action) would not teach or suggest a proposed solution to that insufficiency. Applicants respectfully request reconsideration of the rejections.

Based on the foregoing amendments and remarks, Applicants respectfully request entry of the amendments, reconsideration of the amended claim language in light of the remarks, withdrawal of the rejections, and allowance of the claims.

Respectfully submitted,

T. Noguchi, et al

By: Anne Vachon Dougherty
Anne Vachon Dougherty
Registration No. 30,374
Tel. (914) 962-5910